FAILOVER FUNCTIONALITY FOR CLIENT-RELATED SECURITY ASSOCIATION

FIELD

[0001] The present invention relates to a failover functionality for a client-related security association. More specifically, the present invention exemplarily relates to measures (including methods, apparatuses and computer program products) for realizing a failover functionality for a client-related security association.

BACKGROUND

[0002] In modern communication systems, including both mobile and fixed networks, which are typically IP based, client authentication is often realized via a client-related security association between the client and a specific network element. Accordingly, problems in terms of authentication and, thus, problems in terms of communication relying on a preceding authentication could arise in case of a failure of the specific network element resulting in the failure of the security association.

[0003] In the following, reference is mainly made to 3GPP mobile networks for illustrative and explanatory purposes so as to exemplify the aforementioned circumstances. It is to be noted that, while reference is mainly made to 3GPP mobile networks hereinafter, such reference is made by way of example only, and similar considerations equally apply to other types of mobile networks and/or fixed networks accordingly.

[0004] For example, in IMS- or other SIP-based networks, the SIP protocol is used for session handling. The SIP protocol defines the procedure of registration, which is the linking of the local transport address (e.g. IP address and port) of a client with the publicly known address-of-record (called "public identity" in IMS) of the client. In the IMS, the aspect of authentication is additionally connected with the registration procedure. For authentication, the IMS AKA authentication method is defined, which uses an IPSec connection between the client and a P-CSCF representing the specific network element in charge of authentication. On the IPSec connection, IPSec security associations (SA) are created at the time of registration and refreshed at the time of re-registration.

[0005] When a client is authenticated via the IMS AKA authentication method, the client can only send and receive SIP messages via the corresponding security associations (SA) via which it is authenticated at the network side. When the SA is not available anymore, e.g. due to failure of the specific network element in charge of authentication such as the P-CSCF, the client is not reachable by the network. According to previously proposed solutions, the client as such has to perform a new registration by itself, which new registration is to take place via an alternative network element in charge of authentication such as an alternative P-CSCF, before the alternative P-CSCF or the like can send and receive any message with respect to the client. The new registration by the client as such may be triggered by an unsuccessful attempt of a connection establishment or at least a re-registration by the client itself. That means that, within a re-/registration period (which may range from e.g. half an hour to several days), the client is not reachable by the network, which is an unacceptable amount of time.

[0006] Accordingly, it is desirable to avoid such unacceptably long service interruption in case of a failure of a network element in charge of authentication via a client-related security association.

[0007] That is to say, it is desirable to provide for an improved failover functionality for a client-related security association.

SUMMARY

[0008] Various exemplary embodiments of the present invention aim at addressing at least part of the above issues and/or problems and drawbacks.

[0009] Various aspects of exemplary embodiments of the present invention are set out in the appended claims.

[0010] According to an exemplary aspect of the present invention, there is provided a method comprising providing a failover functionality for a first proxy function in cooperation with a serving function configured for servicing the first proxy function and a second proxy function, wherein the first proxy function has a security association with a client, and the first proxy function and the second proxy function are reachable with the same network address, wherein providing the failover functionality comprises sending data of the security association or data of the security association together with data of a registration of the client from the first proxy function to the serving function upon registering or re-registering the client at the first proxy function.

[0011] According to an exemplary aspect of the present invention, there is provided a method, comprising providing a failover functionality for a first proxy function in cooperation with a serving function configured for servicing the first proxy function and a second proxy function, wherein the first proxy function has a security association with a client, and the first proxy function and the second proxy function are reachable with the same network address, wherein providing the failover functionality comprises receiving data of the security association or data of the security association together with data of a registration of the client from the serving function at the second proxy function, and creating an alternative security association between the second proxy function and the client on the basis of the received data.

[0012] According to an exemplary aspect of the present invention, there is provided a method comprising facilitating provision of a failover functionality for a first proxy function in cooperation with the first proxy function and a second proxy function at a serving function configured for servicing the first proxy function and the second proxy function, wherein the first proxy function has a security association with a client, and the first proxy function and the second proxy function are reachable with the same network address, wherein facilitating provision of the failover functionality comprises receiving data of the security association or data of the security association together with data of a registration of the client from the first proxy function at the serving function, and storing the received data for a registration period of the client.

[0013] According to an exemplary aspect of the present invention, there is provided an apparatus comprising an interface configured to communicate with at least another apparatus, a memory configured to store computer program code, and a processor configured to cause the apparatus to perform: providing a failover functionality for a first proxy function in cooperation with a serving function configured for servicing the first proxy function and a second proxy function, wherein